Health Information ARCHITECTURE

Role-Based Access Control (RBAC) Newsletter

Volume 16 - September 2004

VHA RBAC Program Manager
Chuck Brown
Chuck.Brown@med.va.gov

VHA/IHS RBAC TF Chair
Dr. Robert O'Hara, MD
Robert.Ohara@med.va.gov

VHA Deputy Chief Architect, RBAC Project Manager
Steve Wagner
Steve.Wagner@med.va.gov

VHA Security Architect, RBAC Architect
Mike Davis, CISSP
Mike.Davis@med.va.gov

VHA Security Architect, RBAC Architect
Ed Coyne, PhD
Ed.Coyne@med.va.gov

VHA Software Security Architect, RBAC Project Lead
Amy Page
Amy Page@med.va.gov

VHA/IHS RBAC TF Functional Analyst Lead
Dawn Rota, RN
Dawn.Rota@med.va.gov

Inside this issue:

HEALTHCARE SCENARIO ROADMAP TO INCLUDE LICENSED AND NON-LICENSED HEALTHCARE ROLES

The Veterans Health Administration (VHA)/Indian Health Service (IHS) Role-Based Access Control (RBAC) Task Force (TF) continues its efforts to expand the Healthcare Scenario Roadmap to include licensed and non-licensed healthcare roles for ancillary healthcare departments. Department-specific versions of the Healthcare Scenario Roadmaps will be distributed to ancillary healthcare departments within the Department of Veterans Affairs (VA), IHS and Department of Defense (DoD) for clinician input. Results will be analyzed, harmonized, and modeled in accordance with the RBAC Role Engineering Process with the purpose of deriving standard healthcare permissions. The roadmap is already complete in the identification and representation of clinical activities for physicians and nurses and other licensed roles in clinical capacities.

The Healthcare Scenario Roadmap has been developed during weekly discussions by clinicians on the VHA/IHS RBAC TF initially using the American Society for Testing and Materials (ASTM) E-1986 Standard Guide for Information Access Privileges to Health Information list of "Healthcare Personnel that Warrant Differing Levels of Access Control". The roadmap can function as a foundational tool to assist in defining the scope of the RBAC modeling effort, as well as be utilized as a quick reference of healthcare scenarios. The roadmap presents scaleable management of user permissions in the form of a list of tasks as a healthcare standard.

STANDARDS DEVELOPMENT ORGANIZATION (SDO) ACTIVITY

o HEALTH LEVEL SEVEN

The Health Level Seven (HL7) RBAC healthcare standards effort continued during the 18th HL7 Plenary and Working Group Meeting in Atlanta, Georgia September 26 – October 1, 2004. The RBAC work item was embraced by the Security Technical Committee (TC) whose attendees included VA and Kaiser Permanente Healthcare RBAC TF collaborative representatives. RBAC updates were provided to the Personnel Management TC and the Government Special Interest Group. On May 4, 2004, the Healthcare RBAC TF presented a proposal to the HL7 Board of Directors at the HL7 Working Group Meeting at which time the RBAC effort (i.e., the specification of permission definitions as a healthcare standard) was approved for adoption into the HL7 family of standards. HL7 is the only Standards Development Organization capable of taking the leadership role for a single international healthcare standard for interoperable RBAC.

RBAC Website: www.va.gov/rbac

VHA ARTICLE

Security and Business Rule Separation
17 Sep 2004
Mike Davis

The VHA RBAC TF is investigating minimum principles for defining and logically separating security and business rules. A systematic approach to achieving this separation will be useful for both role engineering and application development.

The RBAC goal of security as a service means that security policies formerly included as part of each application will now be stored in network directories (policy decision points) accessible to applications through standard interfaces. At the same time, business rules will continue to remain within application boundaries. Legacy applications have tended to combine these two together in ways that may make it difficult now to extract or even understand the difference. In a service-oriented framework, the ability to have a set of logical principles to distinguish application-level business and security rules will be a fundamental first step in determining what policies should be considered for RBAC permissions. This separation will also be useful to developers who need to understand what part of the overall security code their application must develop and what they can expect to see provided by the security infrastructure.

VHA's initial approach has been based upon "litmus tests" of security principle and "guidance to developers". These concepts include:

- Isolating security and business functions
- De-coupling security privilege from time-dependent data views (phase)
- Adhering to separation of duty, least privilege and need to know principles

The VHA paper was presented to the HL7 Security Technical Committee for consideration as part of the overall HL7 RBAC engineering process during the recent October meeting. Following further internal review, the draft paper will be posted for open comment in the near future at:

http://www.va.gov/RBAC

RFC (REQUEST FOR COMMENTS)

RFC 3881 "Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications" has been published. It is the result of collaborative work among HL7, ASTM, Digital Imaging and Communications in Medicine (DICOM), and the National Electrical Manufacturers Association (NEMA) / The European Coordination Committee of the Radiological and Electromedical Industry (COCIR) / Japan Industries Association of Radiological Systems (JIRA) Security and Privacy Committee (SPC). RFC 3881 is a basic reference document for the Integrating the Healthcare Enterprise (IHE) "Audit Trail and Node Authentication" profile and DICOM Supplement 95. (IHE is a multi-year initiative that creates the framework for passing vital health information seamlessly - from application to application, system to system, and setting to setting, across the entire healthcare enterprise.)

The RFC document series, begun in 1969, describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written as RFCs. The RFC series of documents is unusual in that the proposed protocols are forwarded by the Internet research and development community, acting on their own behalf, as opposed to the formally reviewed and standardized protocols that are promoted by organizations such as CCITT and ANSI.

For more information about RFC 3881, reference:

RFC 3881: www.ietf.org/rfc/rfc3881.txt
IHE Profile:
www.himss.org/content/files/IHE_ITI_Node_Authentication_Security.pdf